

REMARKS

Applicant has therefore elected to file an RCE with an accompanying amendment.

The Examiner has finally rejected claims 1 and 4-13 as anticipated by Canny. In paragraph 31 of the Examiner's Action on page 7 he argues against Applicant's response that Canny does not teach performing a computation between first and second data, saying in Section 2 of his description Canny says:

"Assume there are n users...". If n is set to 2, then the system in Canny *is* performing a computation between two users' data, since the public aggregate matrix will contain one of the users' data and the second user will be able to compare his data to this matrix (of one set). This same logic covers the arguments for claims 1, 6, and 11-13.

Applicant believes this reasoning and description of Canny to be incorrect as the aggregate matrix contains the data of all users and thus where n is 2 the public aggregate matrix will contain both of the user's data. The examiner's objection is therefore moot as Canny does not show direct computation between the encrypted first and second data. According to Canny where n is 2, a similarity value is computed indirectly, between the first (or second) data, and the aggregate of the first and second data. Nonetheless, claim 1 has been clarified to relate to the direct computation between the first and second data.

In addition, claim 1 has been amended to include the subject matter that the computation is the direct calculation of an encrypted inner product between the first and second data, or an encrypted sum of shares of the first and second data.

Accordingly with reference to point 27 of the office action, as noted previously, the SVD system of Canny teaches that the calculation of the inner product

is between vectors factorised from the aggregate matrix and not between user data vectors being compared directly between each other as per the present invention

Thus even though the server only obtains encrypted data, a similarity value can still be calculated between the data of two users without their identities being revealed to each other.

As such, claim 1 is novel and inventive. The other independent claims have been amended in a similar fashion, and the same points of distinction apply.

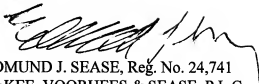
This Amendment accompanies a Request for Continued Examination (RCE). Please charge Deposit Account No. 26-0084 the amount of \$810.00 per the attached Transmittal.

This is also a request under the provision of 37 CFR § 1.136(a) to extend the period for filing a response in the above-identified application for two months from August 22, 2008 to October 22, 2008. Applicant is a large entity; therefore, please charge Deposit Account number 26-0084 in the amount of \$490.00 to cover the cost of the two- month extension. Any deficiency or overpayment should be charged or credited to Deposit Account 26-0084.

No other fees or extensions of time are believed to be due in connection with this amendment; however, consider this a request for any extension inadvertently omitted, and charge any additional fees to Deposit Account No. 26-0084.

Reconsideration and allowance is respectfully requested.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Edmund J. Sease', with a long horizontal flourish extending to the right.

EDMUND J. SEASE, Reg. No. 24,741
McKEE, VOORHEES & SEASE, P.L.C.
801 Grand Avenue, Suite 3200
Des Moines, Iowa 50309-2721
Phone No: (515) 288-3667
Fax No: (515) 288-1338
CUSTOMER NO: 22885

Attorneys of Record

- pw-